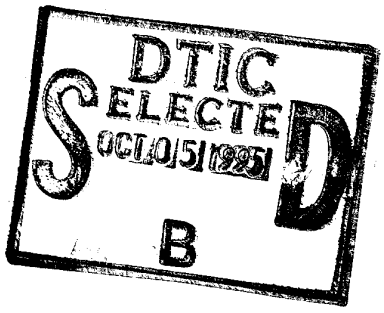
AR-009-248

DSTO-GD-0049

Policy Issues Affecting the Implementation of Public Key Authentication Framework

M.K.F. Lai and M. Anderson



DEPARTMENT OF DEFENCE
DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Policy Issues Affecting the Implementation of Public Key Authentication Framework

M.K.F. Lai and M. Anderson

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-GD-0049

ABSTRACT

The main purpose of this paper is to examine a particular issue which impacts Defence business dealings with other government departments and commercial interests and matters related to national security, specifically those of an economic aspect. While there are many security issues which need addressing, we focus on the near term issue of electronic digital signatures and the need for a regulated, country wide mechanism for the legal acceptance of these signatures across multiple businesses and government organs. Finally, we discus a framework for such a mechanism, namely the Public Key Authentication Framework (PKAF), and expose a number of implications.

APPROVED FOR PUBLIC RELEASE

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury, South Australia, 5108

Telephone: (08) 259 7053
Fax:(08) 259 5619

AR No. 009-248
April 1995

APPROVED FOR PUBLIC RELEASE

Policy Issues Affecting the Implementation of Public Key Authentication Framework

Executive Summary

The rapid advance of new communications technologies under the much touted label "information superhighway" or the more restrained "infobahn", promise to have a marked impact on Australian Society. Recent Government initiatives such as those espoused in the white paper 'Working Nation' [1], are hastening this impact.

While the issues discussed in this paper are intended to deal mainly with matters which will affect the Commonwealth Government as a whole, our basic thesis is that Defence must play an active role in some elements of the development of the infobahn and help shape its direction as early as possible.

The main purpose of this paper is to discuss a particular issue which impacts Defence business dealings with other Government departments and commercial interests and matters related to national security, specifically those of an economic aspect. The issue in question is the use of the infobahn as a medium for conducting business transactions. Legal business transactions imply a means for authenticating the parties involved in the transaction, and ascertaining their agreement to the transaction. The use of the infobahn to carry out these procedures implies secure implementations of digital signatures.

The Public Key Authentication Framework (PKAF), is a proposed mechanism [31] for conducting legitimate electronic commerce by providing an accepted framework for Government and business to check on a digital signature's authenticity. That is, a mechanism is needed with an associated framework so that we may recognise and be able to authenticate various digital signatures locally. However, on being presented with a signature which has not been seen before, it must also be possible to appeal to a trusted source as to the signature's veracity and its association with the specified originator.

By suggesting PKAF, we are seeking a cornerstone on which other trustworthy information security mechanisms can be built for Government wide automated information applications. However, PKAF by itself is unlikely to be suitable for Defence use for national security classified information. With the advent of digital signatures in the commercial arena, Defence nevertheless will have to interoperate with these systems. Hence Defence users will have to have access to the system employed by the vast majority of businesses.

Defence will be reluctant to provide access to military grade technology for general use with commercial transactions. It is also unlikely that Defence will successfully demand a paper-based system in order to maintain a form of traditional integrity. In reality, Defence will be coerced into a position of following the civilian mechanisms when it comes to dealing with entities outside its domain. Accordingly, it is in Defence's interests to influence the development of PKAF or the digital signature mechanisms which are adopted in order to satisfy itself that they are workable for commercial transactions and to minimise difficulties of interoperability with Defence networks.

One conclusion that may be drawn is that Defence will logically have a dual system. It can use the PKAF system when conversing with commercial suppliers or other arms of government, and a military grade system for internal use.

Authors

Lai M.K.F.
Information Technology Division

Dr. Lai received his B.Sc. (Mathematical Science) First Class Honours degree in 1984, followed by his Ph.D. in Combinatorial Group Theory completed in 1987, both from the University of London. He is currently the Senior Research Scientist in the Information Security Section of Trusted Computer Systems Group at DSTO. His interest coincides with that of his employer.

Anderson M.
Information Technology Division

Dr. Anderson graduated with a Bachelor of Science (Physics and Mathematics) and Bachelor of Science with Honours First Class (Computing Science) from the University of New England in 1982. In 1987 he received a Ph.D. in Computer Science from Monash University. He is currently the Head of Trusted Computer Systems Group at DSTO where his main research interests include Information Security and in particular network security devices and Information Warfare.

Contents

1 Introduction

The rapid advance of new communications technologies under the much touted label "information superhighway" or the more restrained "infobahn", promise to have a marked impact on Australian Society. While much of the current discussion has focused on mass market issues involving Pay Television, and related consumer products such as video on demand, other issues, via extant facilities such as the Internet, have started an irreversible trend which will impact the method by which the Commonwealth and its associated organs will conduct business in the future. In fact, recent Government initiatives such as those espoused in the white paper 'Working Nation' [1], are hastening the aforementioned impact.

While the issues discussed in this paper are intended to deal mainly with matters which will affect the Commonwealth Government as a whole, our basic thesis is that Defence must play an active role in some elements of the development of the infobahn and help shape its direction as early as possible. Given the intention to increase use of civil communications infrastructure assets, if Defence does not participate in shaping the development of those assets, Defence's interests will not be adequately taken into account, and we will, in too many cases, be faced with expensive duplication, or re-engineering in order to obtain the benefit of infobahn services which satisfy credible Defence needs. Worse, Defence may be forced into accepting conditions which may substantially increase the risk to our national security due to possible huge expense in achieving infobahn re-engineering.

The main purpose of this paper is to discuss a particular issue which impacts Defence business dealings with other Government departments and commercial interests and matters related to national security, specifically those of an economic aspect. The issue in question is the use of the infobahn as a medium for conducting business transactions. Legal business transactions imply a means for authenticating the parties involved in the transaction, and ascertaining their agreement to the transaction. In the paper world, this has been resolved traditionally by the use of a signature on a contract. The use of the infobahn to carry out similar procedures implies secure implementations of signature equivalents, namely digital signatures[1]. It is expected that an agreed mechanism will be vital for successful commerce in the "bazaar" of the infobahn.

This paper first discusses the importance of the infobahn revolution, and raises the need for good security mechanisms for the safe conduct of business. While there are many security issues which need addressing, we focus on the near term issue of electronic digital signatures and the need for a regulated, country wide mechanism for the legal acceptance of these signatures across multiple businesses and Government organs. Finally, we discuss a framework for such a mechanism, namely the Public Key Authentication Framework (PKAF), and expose a number of implications.

1. Represented in numerals, digital signatures are not the digitisation of hand-written signatures.

This is a blank page.

2 *Arrival of the Infobahn*

Innovations based on information and communications technologies are generating a "new" industrial revolution as significant and far-reaching as those of the past. At the core of this revolution is the evolving infobahns. They are being built with the entrepreneurial motivation of the private sector, and are encompassing advanced infrastructure which will enable us to process, store, retrieve, convert, apply, present and communicate information in any combination of oral, written or visual form unconstrained by distance, time and volume. The arrival of the infobahn is no longer considered as a matter of "if" but "how soon". When the web of information extending from the infobahn reaches many levels of the society, the ways in which we work and live will be changed. It will transform peoples' perceptions and values. There will be new ways for individuals, organisations and even countries to relate with one another through closer collaboration, without regard to geographical boundaries. The potential new wealth, jobs and savings generated from advanced information services supporting production, manufacture, commerce, consumption, culture, leisure and even military activities are considerable if we as a nation properly manage the technologies which underpin the infobahn.

2.1 Defence's Main Interests in the Infobahn

Improved military activity often has not been mentioned as a beneficial factor in public infobahn debates. However, the contributions that a strong and modern C3I (command, control, communications and intelligence) capability can make to an effective and efficient Australian Defence Force (ADF) cannot be stated any more clearly than in the recently published 'Strategic Review 1993' [2] where greater use of civilian technology is given a high priority. Technologies such as those embodied in the infobahn represent levels of functionality not available in extant Defence networks. In addition, Defence is under considerable pressure to make use of the civil infrastructure in order to carry out its corporate downsizing and outsourcing.

2.2 Infobahn Investment- A Global Trend

The first countries to enter the information society created by the infobahn will reap the greatest rewards. They will set the agenda for those that follow. The importance of the business sectors generated by the infobahn, namely computing, communications and information services, was evident by their prominence during the Uruguay round of General Agreement on Tariffs and Trade (GATT) negotiations and is reflected by the decision to postpone access agreements for these specific sectors until future rounds of negotiations [3].

Developed and industrialised countries are investing heavily in high-technology and high value-added goods production sectors in order to be less dependent on labour costs, since they cannot compete with developing countries. Fundamentally, they see these sectors as ones where new jobs can be created at a sustainable rate under the market economy. On the other hand, developing countries see the same sectors as ones which can accelerate their national development and improve their national infrastructures. Generally, they tend to belong to the infobahn end-user community. In other words, many countries believe their future will be significantly affected by the infobahn, but there are wide differences in objectives. The importance of infobahn related sectors is destined to increase. It is therefore crucial that a country must identify its own unique issues before the implementation of the infobahn will decide those issues for them.

2.3 Goals and Policies

Various countries around the world are actively shaping their work practices based on the infobahn. The US began their activities through their President's executive order on the

development of "National Information Infrastructure" (NII) in September, 1993 [4]. Subsequent white papers, proposed new bills and commentaries (most of which are documented in [5]) not only sketch a vision of their future but have also greatly heightened the level of public debate on information technology and social change, most notably in the areas of escrowed encryption of confidential information and also of universal access to the infobahn. European countries are developing their plans collectively through the European Council (EC) as well as individually. The EC has produced a high level document 'Europe and the global information society' [6] identifying ten trial applications on their infobahn to launch the information society. Germany is developing its "Infobahn TeleKom 2000", France is planning its "Great Project" which will encapsulate more than its currently established "Minitel" [5]. Other trading nations, particularly those in the Asia-Pacific region, ranging from a major power such as Japan through to others such as Singapore and the Philippines, are also seeking to realise major social and business objectives through the construction of the infobahn.

Recently, the infobahn concept has entered new arenas in the international fora. At the last G7 meeting in July, leaders from the seven major economies have agreed to hold a ministerial-level meeting, early in 1995, dedicated to the spread of new technologies and the so-called 'Global Information Infrastructure' (GII) [7]. Beginning with the International Telecommunications Union (ITU) plenipotentiary conference in September 1994, similar issues are likely to be discussed in a number of international venues, such as the Organisation for Economic Co-operation and Development (OECD) and Asia Pacific Economic Co-operation (APEC).

2.4 Australian Initiatives

The Australian Government has its own initiative; 'Working Nation - Policies and Program' which was presented by the Prime Minister in May, 1994. This has subsequently been followed by various studies, inquiries, and committees to investigate the issues associated with future infobahn deployment within Australia. They include the telecommunication development inquiry from the Senate Standing Committee on Industry, Science, Technology, Transport, Communications and Infrastructure; the Broadband Services Expert Study Group organised by Department of Communications and Arts; the Australian Science, Technology and Education Council study of Research Data Networks; the Taskforce on Bulletin Board Regulation; Communications Future Project of Bureau of Transport and Communications Economics etc.

Some interim reports produced from these activities are now publicly available [8], [9] and [10]. They all agree that the emerging infobahn has the potential to improve the quality of life of our citizens, the efficiency of our social and economic organisation and to reinforce cohesion. They also identify that Australia has positioned itself well in receiving the potential benefits unleashed by the infobahn. The coverage rate of telecommunication networks in Australia is one of the highest in the world, whether measured by number of homes with telephones, or by the amount of installed optical fibre cable, or by the extent of digitisation. Australia also has a track record of adopting new technologies rapidly, e.g. the fax machine, Video Cassette Recorders (VCR) and mobile telephones. Per capita computer use in Australia is very high, second only to that in the US. High technology literacy among Australians is also very strong compared with other countries. Close to 10% of the population are already enjoying some limited state-of-the-art information services including electronic mail, news, and bulletin boards.

2.5 Issue Priorities and Responsibilities

Based on the recent studies/inquiries mentioned above, a list of issues can be determined for examination in greater detail. This list of issues can be sub-divided into four main categories; namely:

- information - the commodity of infobahn;
- architecture (software, hardware and networks) - the media of infobahn;
- people - the beneficiaries of infobahn; and
- finance - the investment of infobahn.

Because of the size of the list and the potential complexity of each issue, ad-hoc methods of the past for resolving issues are no longer applicable.

Private and public sectors are eager to begin using infobahn elements[2], by either taking roles as vendors, service initiators, service providers or simply as end-users. There are however many uncertainties, including the responsibilities and privileges of users and service providers, and the legality of "electronic" agreements.

It is evident that multiple Government departments and agencies will have their own individual concerns in each issue category. If every department or agency separately addresses these concerns, the net result for Government will be a more fragmented and much less effective amalgam of individual solutions by the departments and agencies.

2.6 Information Security - A Vital Issue for Defence

In the case of Department of Defence, it could be argued that information security is one of the most important issues for the department when considering use of the infobahn. Current Defence policy is to exploit civilian technology as much as possible, and the infobahn represents leading edge technology. However, the security needs, and in particular information security needs of Defence are peculiar and much more stringent than those of many civilian requirements.

As stated in The Defence Corporate Plan 1993-97 [11], the Defence mission is to promote the security of Australia and to protect its people and its interests. National security can encompass not only "traditional" defence but also economic aspects, e.g. the protection of communication assets on which the immediate commercial business of the nation depends. Each has global, regional, and national dimensions. Information networks are now used for device control (e.g. electrical power grids), business transactions (e.g. funds transfer) and many others, as well as Defence C3I. The convergence of information networks into an amorphous entity (the infobahn) via a myriad number of connections and new technology has the implication of making adequate control of the entity a criterion for national security. It is therefore important that Defence address the information security issue from the national security as well as the organisational perspective.

Information is essential for the successful conduct of Australian Defence Force (ADF) operations, and for the control of those operations by higher command authorities and Government. Given the requirements for new functionality in Defence C3I systems being developed, it almost inevitable that Defence will have to rely heavily on infobahn elements to implement some of the new functionality. Hence it is desirable that infobahn requirements take into account at least some of Defence's needs. Just as importantly, a major implication is that Defence may be required to protect the infobahn against various threats. That is, ensure information security from a national security and economic perspective.

2.7 Information Security - A Vital Issue for the Civilian Community

The application of information and communications technologies have been contributing greatly to distributed electronic commercial transactions. The same can also be said for all government departments. However, until recently, Government information and communications strategy has always concentrated on the internal organisation structure. Their systems have largely been closed with no external connections. The working nation paper and

---

2. Examples of some most recent initial enquiries are discussed in Section 3.3.

associated literature implies a myriad number of links between Government systems and commercial entities.

In this increasingly competitive global market place, the most successful businesses are those with a global reach. They design their operations to facilitate the free flow of products, technology, ideas, information and capital to serve their customers more efficiently. They must communicate externally with their vendors, suppliers and customers worldwide. As a result, just as for the military, business is also increasingly demanding seamless communications networks whereby information can flow in a free, timely, and secure manner. Given the increasing importance of electronic information transfer, information itself is becoming more vulnerable as hackers, criminals, and other unauthorised parties find increasingly sophisticated tools to violate the security of communications systems. This has prompted various international strategy planning organisations, including International Chamber of Commerce (ICC) [12], OECD [13] and the European Council (EC) [14] to examine the associated issues of information security. The 1993 European Council Green Paper on information security specifically concluded the following: "The confidence in the security and safety of communication services and systems is a basic requirement. (If not) it might only take one incident to undermine user confidence with substantial financial and political repercussions."

3 *Characteristics of Electronic-based Information*

Information has traditionally been bounded by a single media in which the information was presented. Paper-based information may be referred to as text while we refer to talk or speech as audio-based information. A format is used to represent a piece of information in a media and to retrieve it from the media. Even money is a type of information: it states the purchasing power that the owner of a note or a coin can have. In other words, information is just the abstraction of everyday items that we use for getting things done. Information has an associated value and it can be traded just like any other commodity. However, only quality information can be called "valuable". Good quality information must be secure, timely, user-friendly, appropriate to the recipients, and available via diverse routes. In particular, secure information means that:

- the information is authentic (from an authoritative source);
- the information integrity is maintained so that an unauthorised modification may be detected;
- the information confidentiality is preserved in order to allow only authorised access.

Information handling has always been a part of everyday human activity, in either trading information or inputting information to production or organisational/personal processes:

- government absorbs information to make policy and legislation;
- businesses use information to address market issues and to facilitate the formation of transactions;
- military fuses information to achieve its mission;
- law and order requires information to protect communities; and
- society needs information to evolve and improve its quality of life.

However, handling information based on conventional media (mainly paper-based) has been time consuming and manually intensive, especially when information is required to be transferred from one media into another. Digitisation of information changes the nature of information handling. It allows information to be electronic-based. The information content becomes totally plastic - any message, sound or image may be edited from anything into anything else; an immediate potential compromise of information integrity.

3.1 Information Security and Digitised Information

Information digitisation, as is any other human-invented technology, is a double-edged sword. While it is improving certain aspects of information quality such as timeliness, user-friendliness, and availability, it presents new challenges to assure information security. The major implication of information as a commodity is that it is vulnerable to compromise. This implication is summarised by Estrin and Holmes [15] as follows. "Information, as a commodity, displays economies of scale in production, monopoly power in exchange, positive external effects and public goods and properties in its supply, with incentives for traders to cheat." Consequently, quality and particularly security of information have to be assured depending on its value.

It is difficult to allocate the authority boundaries within the infobahn as it is only the representation of a technological capability for information. Internet is a prime example of a situation where such a technological capability is exploited for commodity purposes. Once input to the terminals and delivered into the networks, the meaning of information ownership is significantly diluted. To date, there are only laws that prevent unauthorised access to computer systems. Laws that prevent access to information within the networks do not exist. In fact such laws are difficult to make practical with current technology as they would contradict the universal access criterion for information services provided by the networks. Moreover, information as a commodity raises interesting legal issues when carriage across authority boundaries takes place.

3.2 *The Legal Standing of Information Technology*

Until now, information technology (IT) has been relegated to the role of assistance in terms of information exchange. In most cases IT-generated information must still be transferred onto paper and then hand-signed, sealed and appropriately delivered if the information needs to meet a particular legal requirement. Without appropriate measures against exposure, digitisation is too vulnerable to compromise to permit consideration of the information it represents as secure information in the legal sense[3]. There is no accepted, legal measure of the integrity of the digital information. The current laws are not sufficient to provide the necessary protection to all involved parties, including end-users, vendors, service providers and carriers. In a recent UK court case pertaining to an accusation of access to an electronic mailbox on a UK email system, the defendants were acquitted on the basis that their conduct did not fall within the then existing criminal law [16].

Security measures for the quality of paper-based information were developed so that the relevant laws could be adequately designed to provide the necessary protection. This has resulted in the special status of documentary evidence in both the common and statutory laws [17]. Analogous measures are also required for the infobahn to guard against unwarranted risk exposure. However, these will depend not only on the individuals involved and their physical environment, but also on the information technology itself.

Although most people support the general goals of information security, there is disagreement with respect to the levels of reliability and security needed, and the extent to which goals of other quality aspects should be sacrificed to achieve these goals. This has resulted in the need for different information security classifications (e.g. Top Secret, Restricted, Highly Protected, In-Confidence) [18] to reflect the value of various information and level of protection afforded it. As a result, the security measures that are being designed must be able to meet the different requirements for different classifications of information.

3.3 *Security Implications of IT Expansions into (Civilian) Business Transactions*

The rest of this section uses a series of readily available recent Australian relevant examples (collected from public newspapers and periodicals between August and October, 1994[4]) to highlight the importance of information security for the infobahn, and bring to the readers' attention the considerable impact which can result if adequate security is not present.

3.3.1 *Internet Commercialisation*

The Internet is now being used for commercial purposes. How does Government protect potential customers who may obtain false information concerning products or services that they wish to purchase? There is no single accepted mechanism which guarantees the authenticity and integrity of the advertised information available on the networks. Just as importantly, there is no accepted mechanism for legally attributing the source of a piece of information or service on the Internet. The chief operating officer and chairman of the US-based Technology Transfer Institute, and chairman of the Computer Science Department, UCLA and chairman of the US National Research Council's Computer Science and Telecommunications Board recently remarked [19]: "We fear if we let the market settle this (Realising the Information Future: The Internet and Beyond), we may end up with solutions that preclude applications from ever arising because the network won't be able to support them."

3. Some legal subject matters that potentially may be affected by the digitisation of information are listed in Appendix A.

4. The large number of examples collected during the short period clearly indicates the wide spread of Infobahn investment in both Government and private sectors.

The vulnerability of the Internet to malicious activity is considerable. Information "packets" from legitimate Internet users may contain their computer user-identifier (i.e. "log-in" name) and their password, and hence hackers need only install a relatively simple "sniffer" program to snatch every password passing through the system each day and then store it for later use.

Users may be able to secure their own networks from intruders by denying all external access. However, as soon as they connect to other networks, they are at risk to other networks' security implementations. Various vendors have made a variety of security offerings thus encouraging a plethora of mechanisms and styles which may not be interoperable, or achieve acceptance across a wide community base.

3.3.2 CHESS (Australian Stock Exchange)

The $35 million Clearing House Electronic Sub-register System (CHESS) for the Australian Stock Exchange (ASX) has just been launched. It is reported in [20], [21] and [22] that when the electronic matching of trading settlements is introduced in 1995 for the large investment institutions, the local exchange will become more efficient. The security related issues have briefly been addressed by the ASX chairman, who has claimed the following [22]: "I can argue that CHESS is more secure but I don't need to because in both cases investors are protected by the national guarantee fund. No investor since the ASX was formed has lost anything on a securities transaction executed on the exchange with a stockholder other than through the movement of the market, and that position is not going to change."

CHESS deals with the risk of compromise by insurance means. However, when Government business is taken into account, or national security for that matter, the Government is its own insurer. There are limited opportunities to transfer the risk. In the case of the infobahn, considerable loss may occur if it is used to conduct Government transactions of a commercial nature in a manner which precludes strong authentication mechanisms for determining whether the transaction is legitimate.

3.3.3 Attorney General's Department and OECD Guidelines

According to Commonwealth Government IT News [23], member countries of the OECD met, in November 1994, for the first time to review OECD's guidelines for the Security of Information Systems. The current guidelines [13], established in 1992, outline nine principles to be considered in protecting information systems and providing for their security. The nine principles are: accountability, awareness, multi-disciplinary, proportionality, integration, timeliness, reassessment and democracy. At that meeting, representatives were required to report progress on the implementation of these guidelines in their respective countries [23]. The responsibility for co-ordinating the implementation of the guidelines in Australia rests with the Federal Attorney-General's Department. It has been reported in [23] that the Australian Government's approach to the implementation of the Guidelines for the Security of Information Systems has been to refer legal aspects to the Australian Government Legal Practice, and to lodge a proposal with Standards Australia for the development of a standard or code of practice to cover the security of information systems.

We believe that the guidelines should be extended to cover information also and not merely information systems. Information will be one of the most important commodities of the future and information systems are a supporting tool for using quality information. Not only is good security required of information systems to maintain the quality of information they hold and process, further mechanisms which can bind quality indicators to the information itself and which are as far as possible independent of the information systems are necessary. Separate stove-pipe systems rated on the integrity of the information they process are ponderous solutions and could lead to restriction of the infobahn to low quality information.

3.3.4 *Government Purchasing by Department of Administrative Services*

The Department of Administrative Services (DAS) has recently called for submissions for development of a strategy and a timely report on electronic commerce system for Government purchasing [24]. This is the result of the White Paper on Employment and Growth which outlined significant changes to the Government's purchasing arrangements. It has been decided by Government to move to electronic commerce over the next three years with initial funding for 1994/95 approved in the Budget. At the same time, the Australian Government is already involved in an international EDI (Electronic Data Interchange) initiative under the umbrella of an APEC arrangement. This initiative started in November, 1993 and its primary objective is to achieve electronic-based transaction capability between suppliers of different countries and warehouses located in different countries. The Australian involvement is coordinated by the Maritime Policy Division of the Department of Transportation.

3.3.5 *A Recent Survey on EDI Deployment*

It has been revealed by a Coopers and Lybrand 1994 survey [25] that 47 percent of our top 1000 companies are using EDI. However, the report also indicates that the majority of the companies that have adopted EDI are still using it only in a small way compared with how they could integrate electronic gateways and other processes into their supply chains. This implies that these companies do not have enough confidence to apply EDI to their mission critical operations, particularly those involving external companies.

While information security technologies can address the security of EDI information content, the current contractual arrangements between EDI users, EDI service providers, and telecommunications carriers, and among EDI users are not adequate in terms of the responsibilities and privileges of users and service providers. ICC (International Chamber of Commerce) currently has a publication titled 'Electronic Data Interchange Agreements' [26] which contains model agreements, and negotiating strategies applicable to the Australian legal system as well as those of other major countries. However, these agreements cannot be universally signed and they are dependent on various trading configurations (e.g. one-to-one or group trading).

As a result of the inability to "electronically" sign documents which may have a requirement to be recognised legally by multiple entities, huge inefficiencies may become apparent. For example, let us suppose that there are n companies who may potentially trade with each other using EDI. Then each company would require a bilateral agreement with each trading partner and a multilateral agreement for each trade group. In other words, the company would require potentially $2^{n-1} - 1$ different agreements. Within the community of the n companies, there can potentially be $2^n - (n + 1)$ agreements. The number of agreements increases exponentially as the number of partners grows.

One possible solution to overcome this inefficiency is a single, accepted mechanism which can cover all potential users and providers of the basic EDI service on a national, if not international basis. This mechanism would allow a user organisation to sign only a single simple agreement which can bind it with the providers and other user organisations for engaging in the basic EDI service. A specific bilateral or multi-lateral agreement is required only if the organisation wishes to have a special arrangement with a particular trading partner or group of partners.

3.3.6 *ICAC Report on Unauthorised Release of Government Information*

Following a series of incidents occurring in 1990, the then Assistant Commissioner of ICAC, Mr. Adrian Roden QC, began an official investigation into the unauthorised release of government information. After a period of two years, it was reported [27] that widespread illegal trade of government information was taking place. More than 250 people were

identified as having participated in the trade, or contributing to it. Information from a variety of State and Commonwealth Government sources and the private sector was freely and regularly sold and exchanged. The amount of money involved in these corrupt activities, was reported in [27] to exceed many millions of dollars. The report emphasised three important areas that needed special attention.

1. There was no consistent policy to determine what information should, and what information should not, be available to the public.
2. Access to information that was ordinarily publicly available, was frequently delayed to such an extent that a parallel illicit trade developed, with greater speed its prime selling point.
3. Information that was held as confidential, was not well protected. Rudimentary precautions have not been taken with the (Information Technology and Computer) systems that have been in place.

It was concluded that more was required than better management and tighter control of government-held information. There must be strong support from the law. It stated that the present criminal law does not directly address unauthorised dealings in government information. It recommended that the principles of law governing the criminal liability of corporations needed to be reconsidered.

The former ICAC Assistant Commissioner was particularly worried by the lack of adequate security for government information protection and registration of access. The report identified it as a factor in the development of the corrupt trade in information. He reported [27] a general laxity in handling and using the personal access codes, and a lack of care in establishing and maintaining the necessary access audit trails. It was also found by the Commissioner's investigation that there were integrity difficulties with the police system. Some inquires produced conflicting results, and in some circumstances it was clear that the computer system, rather than human error, was responsible. It was concluded that the following three points must be addressed adequately:

1. Within all government departments and agencies where confidential information is held, there should be a comprehensive review of current systems. This should involve both a technical assessment of equipment and programs with upgrading where necessary, and a reconsideration of the access presently allowed.
2. Particular attention needs to be paid to practices regarding personal access codes. It is important that this be done with a view to ensuring that when unauthorised access has occurred, the system will provide maximum assistance to those investigating the matter.
3. Work done in this field in the public sector should be coordinated through a central office responsible for computer technology.

As will be seen from later sections, both the second and third recommendations can be addressed by an implementation of PKAF. However, to address the first recommendation fully, it needs a variant of D6 (a DSTO security architecture under development for the ADF [28]) for civilian applications. Unfortunately, that is beyond the scope of this paper and it requires a full study on its own.

3.3.7 N.S.W. Police Service (COPS)

The Computerised Operational Policing Systems (COPS) is an information technology addition to the New South Wales (N.S.W.) Police Service [29]. It consists of a mainframe which is linked to about 4000 predominantly PC-based terminals. This system provides a facility for police to maintain, enquire and report on all "happenings" (including criminal incidents, traffic accidents, fire reports, missing person reports and lost and found property reports). It also provides a tool to maintain and verify intelligence information obtained by law enforcement officers to assist with investigation of crime, and can be used to develop

strategies for reducing future crime. In the phase to be completed in 1995, the system will incorporate warrants, charge and case management. New technology in such areas as on-line fingerprints, mapping, and image processing have also been planned. As far as the authors are aware, it is believed that the security of the system relies solely on the detailed audit trial that could be traced to show who had accessed the system for information. It is intended that the audit trial be used by management to ensure that access to data and data input are authorised.

The issuing of warrants within the system is of considerable importance. The ramifications of having warrants issued without some strong means of authentication, i.e. checking that the warrant has been issued/signed by an authorised person, and preventing electronic 'forgery' of warrants, would be considerable.

Unrelated to the COPS system but related to Police security is a surprising incident where a woman in South Australia has actually been jailed falsely due to a computer system not being updated to reflect a change in status [30]. In fact, a computer system which held data on bail defaulters was not updated correctly resulting in false imprisonment. To quote an extract from the relevant article "Data entry of this nature automatically creates a document, which is then faxed to police. The original document would also be forwarded. However, the police station concerned had no record of receiving the document and the court had no clear proof it was sent".

The aforementioned clearly demonstrates that people place too much trust in computer systems and that much better mechanisms for ensuring the quality of information are needed. In this case, police needed to be able to authenticate data as originating from an authorised entity in a manner which was legally binding. The woman is suing the government for false imprisonment.

We cannot overemphasise that the security mechanisms and legislation developed for paper based documents do not automatically carry over into the infobahn. In the next section, we focus on the authenticity and integrity of information as a discussion point. More precisely, we shall discuss the equivalent to signed documents.

4 PKAF (Public Key Authentication Framework)

Before the 12th century, information was largely exchanged orally. Security depended only on the individuals involved and on the physical environment. After writing material became widely available, signatures, special papers, and wax seals have been considered as the main method and tools for information authenticity[5]. Security, in these cases, depended not only on individuals and associated environment but also on the strength of measures such as signature validity. Traditionally, handwritten signatures have been the most common legally recognised form of document origin authentication[6], guaranteeing both document integrity and non-repudiation. However, it should be acknowledged that a handwritten signature by itself is not perfectly secure and may be forged. Even with the use of special papers and wax seals, we can only increase assurance or confidence of integrity but never achieve 100% integrity[7]. Despite these imperfections, the handwritten signature has gained its current legal status through the gradual evolution of civilisation, which has depended on the physical exchange of information largely contained in some paper-based media.

In all of the aforementioned cases in Section 3.3, one particular electronic security mechanism, authentication of the integrity of transmitted information, comes to the fore as a necessary component for the correct operation of the systems. There are significant changes required to achieve the necessary level of security for authentication of electronic documents.

With the advent of the infobahn the main tool to assure authenticity of exchanged information will be the Digital Signature. Handwritten signatures will remain but become steadily more inefficient and ineffective as an increasing amount of information will be generated, processed and stored electronically. Just as for handwritten signatures, the acceptance of digital signatures will be inevitable. While it is not necessary to impose the acceptance of digital signatures upon society at this point in time, it is important that the foundation should be constructed now so that a smooth and secure transition path is identified.

The Public Key Authentication Framework (PKAF), is a proposed mechanism [31] for conducting legitimate electronic commerce by providing an accepted framework for Government and business to check on a digital signature's authenticity. That is, a mechanism is needed with an associated framework so that we may recognise and be able to authenticate various digital signatures locally, just as we do with handwritten signatures. However, on being presented with a signature which has not been seen before, it must also be possible to appeal to a trusted source as to the signature's veracity and its association with the specified originator.

Although the document is the primary information type to be focused on because of its special legal status, other information types including audio, video and ultimately multi-media can also be covered by PKAF with similar means. Initially, PKAF is intended to be implemented for Government as well as for intra and inter Government departmental communications.

4.1 Technical Foundation of PKAF

While implementations of PKAF can be based on software, firmware, hardware, or combinations thereof depending on specific security requirements, there is a common requirement for all implementations. Namely, they must mutually recognise information handled by others so that a document "signed" by a PKAF user can be properly authenticated by any other PKAF user. These implementations should operate with any messaging facilities available on mainframe terminals, personal computers or workstations connected to networks. In order to achieve a suitable level of assurance that security is maintained, one can envisage

5. These result in the special status of written documents (c.f. Appendix A).
6. c.f. Appendix A.
7. Thus the need for resolution of disputes (c.f. Appendix A).

possibly the use of mechanisms such as smart cards with Personal Identification Numbers (PINs) etc.

4.1.1 Digital Signature Creation

The signature creation mechanisms of PKAF are derived from the type of cryptographic schemes known as "public key" or "asymmetric" schemes, e.g. [32] and [33]. These schemes allow a unique key pair to be associated with an identity of a PKAF user. For each key pair, one key, known as the "private key", is kept private by the associated user or his/her trusted agent while the other, known as the "public key", is made available (preferably electronically) either via some directory service or to specific communities of the user's choice.

It is very important to be aware that the proper use of these schemes and therefore their security depend on the maintenance of the secrecy of private keys. It is also well known from the literature [32], [33] that all the public key or asymmetric schemes proposed for civilian use[8] are not 100% provably secure. In other words, these civilian schemes cannot guarantee that there is no better way of discovering a given private key than what is known as brute force guessing. Regardless of which civilian scheme is chosen, there can be ways of discovering private keys without the knowledge of the key owner and they are widely discussed in the open literature [32], [33]. However, all these publicly known ways of discovering the private key do rely on intensive computations which require either lengthy computing time or/and huge computing power. Hence, the private key secrecy and therefore the proper functioning of a civilian scheme depends heavily on the current lack of computationally-efficient ways of discovering private keys. It is important to be aware that there always exists a non-zero possibility that someone may discover an efficient way of ascertaining private keys with respect to a particular civilian scheme.

While the schemes mentioned above may be suitable for civilian use, military systems are expected to require further assurance for matters of high grade national security.

Through the use of one of these civilian schemes, document (or information) authentication, is achieved from the creation of a "digital signature" which is peculiar to the combination of the document (or information) and the author's (or originator's) private key. Digital signatures created from different private keys are essentially distinct. Integrity is maintained because a modified document (or piece of information) cannot correspond to the associated digital signature of the original, even with the use of a valid private key.

4.1.2 Digital Signature Validation

To validate the true identity of the author of a document and therefore to establish the document authenticity and integrity when dealing with a digital signature, one must have access to the author's public key. A value is computed from the combination of the author's digital signature (w.r.t. the document in issue) and his/her public key. Such a computation is the logical reversal of the signature creation process with the roles of document and digital signature being swapped. Only if the computed value matches that of the document in issue can we then assert that the author's identity is truly valid and the document in issue is both authentic and has not been tampered with. Using either digital signature w.r.t. a different document or a different public key would not produce the same value. Consequently, the author of a document in issue cannot deny the existence of the document. At the same time, a recipient can be protected from receiving a document from a masquerading source.

8. Hence, they are also termed "civilian cryptographic schemes".

4.2 *Why PKAF is Needed*

There are companies who claim to provide security services for electronic transactions over the Internet. In addition to similar authentication provisions covered by the PKAF concept described above, they also supply customers with 'envelopes' in the form of encryption functions. Customers put their information into the supplied 'envelopes' via these functions. 'Seals' of the information are provided by the companies via their digital signatures attached to the encrypted contents. What makes PKAF different from these non-Government-approved mechanisms purporting to supply digital signatures is the provision of trust. That is, there is the ability for one party to approach a trusted authority to verify that a digital signature is indeed associated with the designated originator. Although various vendors offer mechanisms for achieving digital signatures, there is no single accepted mechanism for a company or entity to associate a given signature with its owner. Essentially, as mentioned previously, businesses have to make separate agreements with their associates on the use of a signature mechanism, and the procedure by which a signature is validated as being associated with its owner.

By suggesting PKAF, we are seeking a cornerstone[9] on which other trustworthy information security mechanisms can be built.

Some may argue that not every type of information transmitted requires a digital signature for authenticity and integrity validation. It is stated in [34] that financial information concerning items of total value less than US$25,000 (e.g. small purchases) need not require any special security in US. In fact, the US DOD Acquisition Law Advisory Panel is recommending raising the threshold to US$100,000 [34]. The point here is that a user should be able to choose his/her option at his/her terminal. While US$100,000 is not a large amount to some people or organisations, it may be considered a great deal by a large number of businesses. If PKAF is implemented appropriately, a trusted digital signature function will be available to every user of the infobahn. Applying the function would be no more complicated than hitting a button. The PKAF technology will not limit the user's choice in signing information.

4.3 *A Dual System - Provision for Robustness*

While the PKAF implementations based on civilian public key schemes may be considered suitable for various Government transactions and other commercial business, their security[10] is not absolute. All extant public key schemes rely on a particularly difficult mathematical problem to maintain their security. It is possible that new mechanisms developed by various mathematicians may be constructed which may weaken the effectiveness of a signature scheme over some period of time. While the probability is very low, it is theoretically conceivable that the PKAF system may be compromised. Hence it is wise to consider techniques for rapid "switch-over" of implementations based on mathematically distinct cryptographic schemes if a particular scheme is found to be wanting.

PKAF is unlikely to be suitable for Defence use for national security classified information. However, with the advent of digital signatures in the commercial arena, Defence will at least have to interoperate with these systems. Hence Defence users will have to have access to the system employed by the vast majority of businesses.

One conclusion that may be drawn is that Defence will logically have a dual system. It can use the PKAF system when conversing with commercial suppliers or other arms of government, and a military grade system for internal use. It is possible to see this second military system being used as an emergency backup by the wider community if a compromise is found in the PKAF system. We do not suggest that if a compromise to PKAF occurs then ALL users of PKAF gain access to the military system. Only certain, designated PKAF users who conduct business or

9. See "D6: A Security Architecture for Large, Distributed Multimedia Systems" [28].
10. Discussed at the beginning of this section.

transactions which under the emergency could adversely affect the nation's well-being would have access to the military system in a crisis. An example may be major "trunk" transactions involving many tens of millions of dollars between Government departments, and other highly sensitive material.

4.4 PKAF: Implementation Issues

What algorithm and mechanisms are suitable for implementing digital signatures? The answer to such questions may ultimately be technical in nature but it is at the policy level the question must be asked, and a work program put in place. Clearly, the selected algorithm should be as secure as possible. However, as mentioned in Section 4.1.1, all extant civilian public key mechanisms are not 100% "provably" secure. There is always some risk, however slight, attached to the use of any current asymmetric key system.

Section 92 (1) Subject to subsection (2), it is the duty of a person who is an employee of Australian Post not to disclose any fact or document that:

(a) relates to:

(i) the contents or substance of an article that has been carried by post or an article in the course of post;

(ii) postal or telecommunications services supplied, or intended to be supplied, to another person by Australia Post;

(iii) the affairs or personal particulars (including any address) of another person; and

(b) comes to the person's knowledge, or into the person's possession, because the person is an employee of Australia Post.

(1A) Subsection (1) does not apply in relation to the disclosure by an employee of Australia Post of the name and address of a person ("the customer") if:

(a) the disclosure is made with the customer's consent given in writing on a form obtained from an office of Australia Post; and

(b) the disclosure is made to a person or an organisation covered by the customer's consent; and

(c) the disclosure is recorded by Australia Post.

(2) Subsection (1) does not apply in relation to a disclosure by a person:

(a) in the performance of the person's duties as an employee of Australia Post;

(b) as a witness summonsed to give evidence, or to produce documents, in a court of law;

(c) under the requirements of a law of the Commonwealth; or

(d) in prescribed circumstances.

Section 96 (1) Australia Post's seal shall be kept in such custody as the Board directs and shall be used only as authorised by the Board.

(2) All courts, judges and persons acting judicially shall take judicial notice of the imprint of Australia Post's seal appearing on a document and shall presume that the document was properly sealed.

Figure 1 Some Sections of Australian Postal Corporation Act 1989 [35]

Other relevant questions needing resolution include the following.

- "How will the signature certifying authorities implement their mechanisms?"
- "In what locations should these signature certifying authorities reside?"
- "How robust should the mechanisms for implementing these authorities be?"

Figure 1 depicts legislation concerning Australia Post. It describes obligations and responsibilities of employees concerning mail. A digital signature scheme which is in use by the wide community would require similar trust requirements on those employees of the certifying authority. Hence while the selection of algorithms and structure of the certifying authority are important, it is equally important to ascertain those areas which require the highest degree of trust and develop both technical and procedural mechanisms which minimise the risk of illegal exploitation of positions of trust.

4.4.1 Archiving and Public Document Records

Just as a user's PIN on their credit card may be inadvertently exposed, it is possible for a user's private key to be exposed. Hence it is reasonable to expect that users will periodically wish to change their public and private keys. Doing so however, changes their corresponding digital signature. Consequently, other PKAF users would then have to ask one of the PKAF certifying authorities whether the new signature is a valid representation of the claimed owner. While this is one of the main reasons for PKAF's existence, there is another issue which arises and it is called the archiving issue. Public documents and their records are intended to be long-lived (c.f. Appendix A). If a user's digital signature changes, how does one ensure that long-lived documents signed with old signatures can be verified? Basically, an archiving mechanism is needed so that when PKAF users inspect documents which may be "old", it is possible to check that the signature was valid at the time it was signed.

In order for such an archive to work, it would have to store user private portions of the keys used to generate the signatures at the time of signing. This would allow the originator of an archived document to retain his/her ownership over the document. However, if the originator does not wish to retain ownership, the Archival Authority could issue an accompanied statement that the originator's signature associated with the archived document has been "checked" at the time of archival. The signature of the Archival Authority would then be attached. The archive would have to be an extremely secure entity. Compromise could mean retrospective forgery of documents.

A major issue is who will act as the Archival Authority? What executive responsibility will they have? How will law enforcement agencies gain access to private key parts in the performance of their duties?

4.4.2 Management

If PKAF were brought into being, the question arises as to who will manage the certifying authorities? Clearly, the management entity would have to have a great deal of credibility and trust with the PKAF user community: the electronic funds transfer system could well depend on the integrity of the management entity.

At first glance, it is tempting to nominate the Defence Signals Directorate (DSD) as the management entity on the basis they are the National Computer and Communications Security Authority, and they are responsible for provision of key material for the nation's high grade crypto systems. However, simply attempting to designate DSD as the management entity without further consideration would be naive in the extreme. DSD, a department of defence entity, is not established or resourced to manage the security of the nation's economic transactions. It would seem ludicrous to burden a Defence entity with the task of storing, say, the archives of signatures and delivering them on request. Such a function is well outside their core business. However, as the national computer security authority, it may be more appropriate

to regard DSD as a source of key material, and as an adviser on the suitability of algorithms proposed for use by PKAF.

It is the authors' view that neither private enterprise, nor any Government department (given their current functions) seems to be the "natural" location as the management entity. It may be suggested that the management entity should be collocated with those departments which would benefit most by the PKAF framework. The authors, in discussing the role of DSD, should not be regarded as attempting to influence the debate in any particular direction, but rather as stimulating debate on the management topic by pointing out arguments which show that the issue is not easily resolved.

4.5 Defence interest in PKAF

Defence does business with other government departments and numerous commercial entities; hence when (not if) these entities move to a digital signature scheme how does Defence interact? Clearly, Defence will be reluctant to provide access to military grade technology for general use with commercial transactions. In addition, it is unlikely that Defence will successfully demand a paper-based system in order to maintain a form of traditional integrity. In reality, Defence will be coerced into a position of following the civilian mechanisms when it comes to dealing with entities outside its domain. Accordingly, it is in Defence's interests to influence the development of PKAF or the digital signature mechanisms which are adopted in order to satisfy itself that they are workable for commercial transactions and to minimise difficulties of interoperability with Defence networks. As previously indicated, it is unlikely that the civilian mechanisms will be appropriate for Defence use with respect to high grade classified material.

Defence Science and Technology Organisation (DSTO) are developing a Defence wide security architecture [28] in a project called "D6". Part of the architectural definition describes a possible method for interoperating with commercial suppliers and service providers while still retaining a system suitable for National Security use.

5 *PKAF: Legislation*

The majority of users of communications and information technologies do not require or wish to learn the detailed technology associated with information security. Their main interest is information usage in assisting their organisational and personnel activities. Most of them include security in their requirements but cannot achieve it by themselves. They must rely on an entity who provides the security service and the coordination with other communicating parties. They need to be assured that the ability and professionalism of the service providers are maintained. They also prefer that other parties would respect the security of information [11] in the same way as they do.

While security mechanisms are designed to protect information, corresponding legislation must be available to enable involved parties to gain the mutual trust (authentication) needed to transact their business. In other words, there must be sufficient legislation to clearly define the respective obligations that must be taken and the respective rights that must be possessed by the entities who deal with the security mechanisms. These entities generally include users of security services through the mechanisms and security service providers who operate the mechanisms and administer the services. This implies that the relevant legislation must specify the legitimate relationships between user and user, between user and service provider, between service provider and service provider, and, last but not least, between service provider and the State. Without establishing trust between entities through legislation, users may not be confident that wrongs may have an avenue of redress if very important transactions are involved (c.f. Sections 3.3.1 and 3.3.5).

5.1 The Right Balance

It may be argued that digital signature standardisation could place another burden on the Government's scarce resources. However, one may argue that the resource spent on digital signature standardisation is minimal when compared with the resource that would be required to enforce legislation designed to cover a multiplicity of information integrity offerings, or investigate criminal allegations from users, service providers or State if suitable legislation is not available. The main problem is that every party who has an involvement in information and communications technologies may be liable for a security compromise of information if a trace of the compromised information can be found in the party's domain. Current privacy legislation [36] is not adequate to address the information security discussed in this section. Government should consider the establishment of information security legislation as a parallel to privacy legislation. However, in doing so, the appropriate levels of skilled Government resource, sufficient legislative standards, legislation enforceability, variation of service applicability and user flexibility must be carefully balanced.

11. namely, the information authenticity, integrity and confidentiality, c.f. Section 3.

This is a blank page.

6 Conclusion

The arrival of the infobahn will inevitably link the main elements of business and government. Its pervasive nature will make its protection and control a criterion for national security. The infobahn will form a backbone for business transactions, as well as serve as a major communications conduit for Defence elements. Hence all of the facets of information security will form significant issues which will require resolution.

We have indicated a requirement for legislative or regulatory support for the infobahn to cater for information integrity, and have used the issue of document authenticity and digital signatures as a case in point. Subsequently, we have supported the notion of the PKAF framework proposed by elements in HQADF as a serious contender for dealing with commercial transaction issues.

DSTO, through its D6 security architecture project [28], seeks to develop an architecture to allow Defence to make better use of civil assets, and conduct business with non-Defence entities without compromising sovereignty.

This is a blank page.

7 References

[1] 'Working Nation - Policies and Program'. Australian Government Publications, May 1994.

[2] 'Strategic Review, 1993'. DPUBS, Defence Centre, Dec. 1993.

[3] Wieczorek N., 'The Uruguay Round and the Next Agenda for Global Trade'. Draft general report. Economic Committee, International Secretariat, North Atlantic Assembly, NATO, May 1994.

[4] (US) Federal Register, Presidential Documents, Executive Order 12864: United States Advisory Council on the National Information Infrastructure, Washington, DC, Sep. 1993.

[5] 'Information Infrastructure Sourcebook'. Center for Science and International Affairs, Science, Technology and Public Policy Program, Harvard University, Dec. 1993.

[6] 'Europe and the Global Information Society'. Recommendations to the European Council. Brussels. May 1994.

[7] 'World Infohighway Takes Shape'. Communications Week International - The Newspaper of Global Networking. Jul. 1994.

[8] 'Networking Australia's Future'. The interim report of the Broadband Services Expert Group. Jul. 1994.

[9] 'The Networked Nation'. Draft final report. Australia Science, Technology and Education Council (ASTEC). Jul. 1994.

[10] 'Emerging Communications Services: An Analytical Framework'. Work in progress paper No.1. Communications Futures Project. Bureau of Transport and Communications Economics. 1994.

[11] 'The Defence Corporate Plan, 1993-97'. DPUBS., Defence Centre. Aug. 1993.

[12] 'ICC Position Paper on International Encryption Policy'. Commission on Computing, Telecommunications and Information Policies. International Chamber of Commerce (ICC). 1994.

[13] 'Guidelines for the Security of Information Systems'. Organisation for Economic Cooperation and Development (OECD). 1992.

[14] 'Greenbook on the Security of Information Systems'. Draft 4.0. Commission of the European Communities. Oct. 1993.

[15] Estrin and Holmes, 'French Planning in Theory and Practice'. London: George Allen and Unwin. 1983.

[16] 'Lawyer Warns of Legalish Potholes'. Pacific Computer Weekly. 26 Aug. 1994.

[17] Gillies P., 'Law of Evidence in Australia'. Second edition. Legal Books, Sydney. 1987.

[18] 'Security Guidelines for ANZ GOSIP 3'. Draft. SAA HB55.X:1994. Australian Information Exchange Steering Committee. Aug. 1994.

[19] 'Overhaul of Internet a Must - US Pioneer'. The Australian. Tuesday 6th Sep. 1994.

[20] 'Exchange Opens with a Safe Move'. The Australian. Tuesday 22nd Jul. 1994.

[21] 'CHESS is a Good Move for ASX: Lavarch'. The Australian. Tuesday 13th Sep. 1994.

[22] 'CHESS Endgame to Cost ASX $35m'. Financial Reviews. Tuesday 13th Sep. 1994.

[23] 'OECD Guidelines for the Security of Information Systems'. Commonwealth Government IT News. Vol.5, No.3, Jul. 1994.

[24] 'Call for Submissions: Purchasing Australia - Electronic Commerce System for Government Purchasing'. Department of Administrative Services (DAS). Appointed facilitator: ETC Electronic Trading Concepts Pty Ltd. Sep. 1994.

[25] Integrated Electronic Trading Forum. AIC Conferences. Sydney. Sep. 1994.

[26] Boss A.H. and Ritter J.B. 'Electronic Data Interchange Agreements, a Guide and Sourcebook'. International Chamber of Commerce Publication No.517. 1994.

[27] 'Roden A. QC 'Report on Unauthorised Release of Government Information Volume 1'. Independent Commission Against Corruption (ICAC). Aug. 1992.

[28] 'A Security Architecture for Large, Distributed Multimedia Systems'. Defence Science and Technology Organisation Task Plan ADF93/256. N8316/8/17. Feb. 1994.

[29] 'COPS Go on Line ...'. The Australian. Tuesday 16th Aug. 1994.

[30] 'Woman Jailed Twice from Clerical Error'. The Sunday Mail. Sunday 16th Oct. 1994.

[31] 'Electronic Data Interchange - Digital Signature Facility'. Communications from Information Exchange Steering Committee (IESC). Ref. 92/2486. Nov. 1993.

[32] 'Contemporary Cryptology, The Science of Information Integrity'. Ed. by Simmons G.J., IEEE PRESS, The Institute of Electrical and Electronics Engineers, Inc., New York. 1992.

[33] Schneier B. 'Applied Cryptography: Protocols, Algorithms, and Source Code in C'. John Wiley & Sons. 1994.

[34] 'Electronic Commerce / Electronic Data Interchange in Contracting'. Deputy Under Secretary of Defense (Acquisition Reform), (US) Department of Defense. Sep. 1993.

[35] 'Australian Postal Corporation Act 1989'. Oct. 1992 and 'Transport and Communications Legislation Amendment Act 1993'. No. 4 of 994.

[36] 'The Federal Privacy Act'. Jan. 1989.

Appendix A :

Some Current Legal Views of Evidence Based on Different Media

The following lists some current legal views of evidence based on media other than that represented by the infobahn. They are collected by extracting relevant issues discussed in [17] and page references below relate to that source. We believe that these current views on evidence may potentially be affected or put under pressure by the digitisation of information which has the ability to treat information content as plastic (c.f. Section 3). Although there is legislation concerning evidence obtained from computers, it appears that it is based on the assumption of the past decades that computers are stand-alone devices or belong to a closed network under the control of a single authority. However, the trend of information technology is towards open networks and highly distributed environments. Computers that perform information processing need not be collocated with the user who makes the request and feeds in the initial data. It is most likely the case that both processing and processed information would traverse a number of open networks between the requesting user and processing computers.

1. Page 330. A plethora of statutory exceptions to the hearsay rule are found in Australia. They relate to written rather than oral statements, and more recently to statements recorded in another physical form, such as a computer print-out, photocopy, or micro-film.

- **Photographs**

1. Page 35. Photographs of persons, object or scenes are admissible as evidence of the appearance of the things recorded in them, including inferences arising from these appearances.
2. Page 35. The photograph must, however, be authenticated, viz., there must be evidence that it has not been tampered with, but taken from unchanged negatives. Further, its relevance to the issues must of course be proven by an appropriate witness. ... Once authenticated, a photograph may be admissible as secondary evidence of a physical thing which is an issue.

- **Movie Films**

1. Page 36. Movie films of relevant scenes or activities are clearly admissible according to the same principles as photographs, given that a movie film is but a series of still images. ... The same safeguards will need to be applied as in the case of still photographs, and the relevance of the film will need to be established.

- **Video**

1. Page 36. The principles governing video recording of visual images are exactly the same. the only difference between a video and a film is the method by which the images are stored (the video storing them electronically). It follows that the same general restrictions of the use of films as evidence apply to the reception of videos. Thus, video evidence of an event or thing in issue is not hearsay but real evidence of this item, and equivalent thereby to a photograph. Testimony based on the viewing of a video (including one which has been erased), is of the same status of testimony based on the direct eye-witness viewing the scene.
2. Page 38. A voice on a tape can be identified in various ways, such as by a person who knows the alleged conversationalist, or by an expert in spectrographic voice analysis.
3. Page 298. A video-tape is not hearsay evidence but direct, real evidence of the matters recorded on it, in the same manner as photograph. A witness who has viewed a video-

tape can testify as to its contents (such as where it has been inadvertently erased), without offending the hearsay rule.

- **Audio**

1. Page 37. Tape-recordings - or strictly, the sounds generated by their being played on appropriate equipment - are admissible into evidence as evidence of the fact that the sounds recorded on them (most obviously conversations) took place. Reliance on them as evidence of the truth of matters asserted in conversations recorded is restricted of course by the hearsay rule.
2. Page 37. The tape-recording is analogous to the photograph or movie film. It locks away an event for the purpose of reproduction. Like these other reproductions, where they are sought to be admitted into evidence, the tape-recording must be authenticated by a witness, the voice on it identified, and its relevance to the issues established.
3. Page 37. If it is accepted that a tape-recording is not a document, which today is the preferred view there is no objection to reception of a copy of a tape, provided that it is authenticated.
4. Page 38. In the normal case the only evidence which is admissible is the sounds generated by the playing of the tape - in colloquial if not technical sense this is the "best" evidence - and that as such the transcript is not admissible (either in lieu of the tape or as a supplement to it).
5. Page 38. If a tape is not available and its absence has been satisfactorily accounted for, the evidence of its contents given by a witness who heard it played may be admitted as secondary evidence.
6. Page 38. Once a tape-recording conversation is admitted in a jury trial it is of course for the jury to determine whether it is indeed an authentic and complete record and if so, what interpretation is to be placed on it.
7. Page 38. The tape-recording of a telephone conversation is admissible on the same basis that a tape-recording of a face-to-face conversation is admissible.
8. Page 38. Evidence of a telephone conversation may be given on the same basis as evidence of a face-to-face conversation. This evidence will be given by one or both of the participants, or one who overhears one or both of them. As well, a tape-recording of a phone conversation may be received into evidence. In either case, a witness will have to identify the party or parties whose words are in issue, and make clear the relevance of the conversation.
9. Page 39. Of course, a conversation, whether conducted on the telephone or otherwise, cannot be received as evidence of its contents, unless it falls within an exception to the hearsay rule, such as where it is part of the *res gestae*, or represents a criminal or civil admission by a party to the litigation in question.
10. Page 39. The admission of evidence of conversations carried on through parallel media, such as two-way radio, would logically be governed by the same principles.

- **Computer**

1. Page 39. The term "computer" covers a broad range of instruments, ranging from the simple pocket calculator onwards. Such devices are concerned with the electronic processing of information, taking the form of straightforward arithmetical calculations, or tabulation of data, or more complex analyses of information. Usually, the analyses of results are recorded in the so-called print-out, which document, or testimony based on it, is sought to be admitted into evidence. The print-out, and in turn the data recorded on it, may be admitted both pursuant to common law principles and statutory provisions in each jurisdiction. Where an instrument does no more than store information, which may be retrieved from it in a totally unaltered way, this information may in principle be proven according to the general principles governing the reception of tape-recordings, for these likewise lock away information in unaltered or unprocessed form. The computer-evidence

provisions in legislation may in a particular case of this type also ground admission of this data.

2. Page 361. Such instruments are concerned with the electronic processing of information, from simple arithmetical computations, to tabulation of data, or more complex analysis of information. The typical computer records permanently the results of its analysis in the so-called print-out, and it is this document which is frequently sought to be admitted in evidence. Such evidence is admissible both at common law and pursuant.
3. Page 330. This legislation is significant. It tends to focus on the creation of documents and on devices, such as the electronic storage of information which is printed out by a machine, in the routine process of recording of information in a systematic way, when this information is fresh rather than stale in the memory of the person who acquires it. In admitting this record of information the legislation operates to admit documents as proof of the facts asserted in them, by way of exception to the hearsay rule, which have been created in such circumstances as to enhance their reliability as evidence.
4. Page 362. The print-out or similar computer generated evidence is admissible as the truth of the facts recorded in it, on several common law bases. One view is that it is, essentially, a class of real evidence, and not hearsay, reflecting its status as a mere tool which does not create its own original knowledge. If it is not within the scope of judicial knowledge, i.e., in respect of which a presumption of accuracy arises, subject to proof of accurate reading, a given computer can so to speak be transferred to that class upon proof by expert testimony that is within a class which is accepted to be accurate, and that if handled properly it would have produced an accurate result. In these circumstances, upon the laying of a foundation which, in essence, authenticates the print-out, a "latent presumption of accuracy" arises.
5. Page 363. The typical business records provision provides for the admissibility of records created in the course of business by a person falling within a specified class, who has personal knowledge of the matters recorded, or who is replying upon information supplied by a person within this knowledge. The basis for applying such legislation to computer records is that the computer is used as the medium, or instrument, for the creation of a business record by a person falling within the specified class. The computer, that is, is the mere unthinking extension of the human record creator. The computer records must, however, be created in circumstances which satisfy all the tests specified in the legislation. For example, the Criminal Evidence Act 1965 (Eng.), s.1, provides for the admissibility of a document relating to any trade or business and compiled from information supplied by persons having or who may reasonably be supposed to have personal knowledge of the matters dealt with in the information they supply. The Court of Appeal has explained that this standard business record provision requires the operator to have personal knowledge of the matters covered in the computer output. This is possible where the computer is programmed to do no more than record data fed into it, for the operator (or, in the collective sense, the operators) will have knowledge of the matters fed in and thus of the matters printed out. It is otherwise, the court explained, where the computer analysed the information fed in and after a process of synthesis printed out facts not originally fed in by the operator.
6. Page 362. Specific statutory provisions are found in most of the jurisdictions dealing with the admissibility of computer-generated evidence, which either apply the general business records legislation in them to computer-produced recorded, subject to any conditions spelt out, or provide a unique regime of principle governing the admissibility of evidence of this type. The latter provisions, as a very general comment, provide for the admissibility of computer-produced documents, etc., where the computer output has been produced in circumstances rendering it an inherently reliable record of the information contained in it. These circumstances include reliability of the input, reliability of the instrument, lack of reasonable cause to suspect malfunctioning, adequate supervision of the processing of information by it, competent people to supervise the processing, lack of reasonable cause to suspect improper processing, systematic processing carried out in the routine course of

business, etc.

- **Documentary Evidence**

1. Page 343. The provisions centre upon the concept of a document embodying a statement. In some cases, it has been noted, the legislation in question provides for a (generally) non-exhaustive definition, or interpretation of the term "document". At common law, the term has had to be interpreted in a variety of contexts, including this one. It is clear that a document need not be in paper form - a notation on marble, metal, etc., is capable of amounting to a document. It has been said that a document must take the form of visible writing, whatever the medium, although there is Australian authority to the effect that a tape-recording constitutes a document, because it is a permanent or semi-permanent record of information.
2. Page 575. The terms of a document must, when their meaning is in issue, be established, *prima facie*, in conformity with the best evidence rule. The best evidence rule provides, or provided, that the best evidence which is available must be adduced. As applied in its residual form, it requires the content of a document to be proved by the tendering of the document itself, i.e., the original of this document.
3. Page 574. At common law, the concept is not confined to a notation on paper or a like medium, such as parchment - it can include, for example, an inscription carved into tombstone, or a bracelet. The dominant view is that irrespective of the medium on to which a message is inscribed, the inscription must take the form of visible writing or other figures. It follows that a tape recording is not a document, at least at common law, nor is a video tape. Furthermore, for the purpose at least of the best evidence rule and its associated secondary evidence rule, an item upon which is inscribed a writing (words, figures, numbers, etc.) is a document only when it (or other evidence of it) is sought to be admitted concerning the meaning communicated by these words, etc., as distinct from admission for some other purpose, such as where its appearance is significant.
4. Page 300. It was commented that the legislation "is of great importance in the search for truth. Any significant organisation in our society must depend for its efficient carrying on upon proper records made by persons who have no interest other than to record as accurately as possible matters relating to the business with which they are concerned. In the every-day carrying on of the activities of the business, people would look to, and depend upon, those records, and use them on the basis that they are most probably accurate. This position applies to hospitals, as to any other form of business ... ". It is because of the inherent reliability and importance of evidence consisting of routinely recorded information, that the courts have constantly stressed liberally or broadly, i.e., in a manner favouring the admission of disputed evidence. This is not to say that the weight to be given to this evidence cannot be challenged by other evidence, such as evidence casting doubt upon the circumstances of the creation of the written statement in issue. The legislation of this type does, of course, create a potential danger. Given its systematic creation there is no doubt a tendency to place considerable weight upon evidence admitted by it, but it can only be as good as the information originally supplied.
5. Page 349. A standard provision in some jurisdictions is to the effect that in deciding whether to admit the statement the court may draw any reasonable inference from the form or contents of the document, or from any other circumstance. Pursuant to this the court may have regard to whether the maker signed the statement, or had personal knowledge of it; or a newspaper article relevant to the document.
6. Page 322. A postmark on a letter, etc., is evidence of the place of its posting. It is not, however, evidence that the addressee procured its posting. The basis postmark rule is justified on the basis that the national and international postal systems are organised and run on a systematic basis and that as such the postmark is inherently reliable evidence of place of posting.
7. Page 573. A major general rule concerning documentary evidence is the so-called best

evidence rule. This rule in its pristine form stipulated generally that the best, or most direct evidence of a disputed fact had to be led in preference to other evidence. Today, it applies only to documentary evidence. The effect of it is that the original of a document, the contents of which are sought to be proven for a purpose over and above its identification, per se, must be produced, rather than a copy, or other (for example parol) evidence of its existence and terms.

8. Page 582. The best evidence rule, in its residual area of operation, applies only to proof of the contents of documents, where these visible writings are sought to be relied on for their meaning. It follows that the existence of a document, in the past or presently, may, like any other fact, be proven by secondary evidence. For example, a will destroyed during the lifetime of a testator by factors beyond his or her control may be proven by secondary evidence.
9. Page 319. Pursuant to the *res gestae* principle, the declarations or statements forming part of or constituting an incident in the transaction which in all of its parts and details is a fact in issue, are admissible. These are statements which are so intimately bound up with the transaction that they are inseparable from it and explain its character or (where it is a deliberate human act) its motive or object. These statements must be contemporaneous with the transaction - in essence, they must be a spontaneous reaction to it, so that the implication that they were concocted by the maker after consideration is rebutted.

- **Copies and Reproductions**

1. Page 350. Provision is made in some of those statutes expressly for the reception of copies of documents which would themselves be admissible pursuant to this legislation, subject to conditions specified. The cases establish that a carbon (copy) made at the time an original is created, is readily admissible whether or not there is statutory authorisation for this, the carbon copy being in effect a duplicate original. A copy of a document made after the creation of the document is not admissible pursuant to legislation of this type, in the absence of statutory authority. A provision rendering admissible (subject to the tests) a certified true copy, is satisfied by, in the case of a book, the publisher's relevant statements on the title page.
2. Page 36. Reproductions of documents, by way of photographs, photocopies or microfilms, or by virtue of an analogous process, will in general be sought to be admitted as evidence of the contents of these documents. Problems may be caused by the operation of the best evidence rule, which today is applicable only to documents.

- **Admissibility and Weight**

1. Page 369. Most of the statutory provisions which admit documentary or like statements pursuant to the hearsay rule state that the document shall be evidence, or *prima facie* evidence of the matters contained within it. These standard formula mean exactly the same, viz., the fact of admission says nothing of weight, which may be slight or great and in any event is a matter for assessment by the tribunal of fact. It follows that unless the statute stipulates or implies the converse, the certificate or other document admitted pursuant to it can be challenged by evidence directed essentially to showing that the fact recorded in it did not in fact exist, or was recorded wrongly, or that for some other reason little or no weight should be attached to it. Some of the legislation provides expressly or impliedly that a foundation must be laid for the reception of the documentary evidence in question.
2. Page 369. The document, or other statement, is evidence of the facts asserted in it, but the weight to be attached to it is entirely a matter for the tribunal of fact. This analysis follows inevitably from the basic distinction in the laws of evidence between the questions of admissibility (being for the judge or other presiding officer) and weight (being for tribunal of fact).
3. Page 349. The general law draws a distinction between admissibility and weight after all, with the question of weight being one for the tribunal of fact rather than for the presiding

judge or magistrate, and accordingly of no relevance in assessing whether this evidence is admissible. (There are exceptions of course, as in the case of the discretion in criminal cases to exclude evidence which although admissible, is of only slight probative value but is of serious prejudicial impact.) This, by and large, is the approach which has been taken by the courts, its derivatives and parallel provisions: the lack of weight of documentary evidence sought to be admitted pursuant to the statutory provision is not a factor in assessing its admissibility.

- **Recording and Records**

1. Page 322. Legislation has made specific provision in respect of books of account and like documents, and business records, in most jurisdictions.
2. Page 345. The concept of record is the expansive one, and does of course include, without being confined to, continuous records. A record is a register of information which has been deliberately created for the purpose of preserving this information. It is, therefore, more than just a file of correspondence, such as a business's letters of a single document. It has been held that a document which sets out the history of a transaction for preservation for whatever period is commercially (or otherwise) necessary, can be a document - as will a bill of lading, or a cargo manifest. This case indicates that the document does not have to be created *ab initio* for purely record-keeping purposes, for clearly these documents have other roles as well, such as effecting a transaction.
3. Page 322. In a ruling in the Federal Court a member of that court has suggested that the principle enunciated in the cases dealing with company financial records, viz., that they are admissible because their systematic compilation makes them inherently reliable in respect of broad propositions about a company's financial progress, can be relied upon to support the admission of minutes of the meetings of an unincorporated body complied in a proven systematic way.
4. Page 322. It has been established in Australia that at common law the books of account and other related records of a company (and presumably, an unincorporated business) may be tendered in evidence, along with testimony by a qualified person (such as an accountant) based upon them, in order to establish the financial progress of the business entity in question. A foundation for reception of this evidence must first be laid, by proof that these financial records were complied in a systematic way, viz., according to an established system, for such a method of compilation renders it more likely that the figures are accurate.
5. Page 346. The document or documents, to be a record, must represent the primary or original source of information. It follows that the mere digest of other records (such as a summary of recorded techniques and results of medical research) is not a record, and a document representing not a simple recording of information supplied, but a selection from information supplied, along with opinions - such as a company inspector's report - is not a record.
6. Page 317. The record must be created to be retained indefinitely. Recent English authority holds that the acquiring of information by the officer and its contemporaneity going to weight rather than admissibility. The person who records the information and the person who makes available the document recording it, do not have to be one and the same.

- **Public Documents**

1. Page 368. The common law recognises a public document exception to the hearsay rule, which, when examined, may not be of the same scope as a particular statutory provision. The statutory provisions deal with a wide variety of public documents, such as statutes, regulations, government Gazettes, foreign laws and judgements in and out of the jurisdictions. Other matters covered include certified extracts of registers of births, marriages, and deaths, telegraphic messages, reproductions of documents, welfare officers' reports in the context of child welfare proceedings, certificates as to a driver's blood alcohol content, analysts' certificates as to the nature of a drug; evidential effects of signs on commercial

buildings regarding proprietorship of the premises, certificates attesting to the fact that third party insurance policies were in effect on a given date in respect of given motor vehicles; and certificate attesting to the accuracy of a radar speed analyser.

2. Page 315. At common law a statement in a so-called public document may, by way of exception to the hearsay rule, be admitted as evidence of the truth of the facts asserted in it. This area is now partly covered by statutory provisions in the Australian jurisdictions (the statutory provisions apply mainly to civil proceedings and to criminal proceedings in only limited instances) but the common law public documents exception still finds application in cases not covered by this legislation.
3. Page 315. The justifications for the rule are firstly, convenience and, on occasions, necessity - were it not to exist the person who prepared the public document would have to be called so that he or she could depose personally as to the truth of the facts stated in this document, assuming that this person could be identified and was available; and secondly, the inherent reliability of these documents, which will have been prepared routinely pursuant to a public duty. To the extent that the officer is not required to have personal knowledge of the facts recorded in these documents, this second rationale breaks down.
4. Page 316. These public documents are in the nature of records, given the tests governing their identification. The classic example would be a register of births, marriages and deaths, or data on public file at a company's office, or a Registrar-General's office. Certified copies of public documents are admissible on the same basis as the original.
5. Page 316. A public document is one made by a public officer pursuant to a public duty to inquire and record certain facts for a public purpose, which record is available for public reference.Today, this duty will often be a statutory one. The concept of public officer is not confined to a person in the full time employ of the Crown - a person who, while not in this category, is charged with a relevant public duty is in principle a public officer for the purpose of the rule.
6. Page 316. The requirement that the document has been prepared for a purpose involves, according to one New South Wales case, that a plan or map of land prepared on behalf of a private person does not become a public document simply because it is lodged in a land registry (the New South Wales Registrar-General's Department).
7. Page 316. A document, if it is to have the status of public document, must be created (in part) for the purpose of public reference, viz., the public must have guaranteed access to it.
8. Page 316. Details of companies required to be submitted to a companies office and embodied by that office in a register of company documents maintained by it for public reference, become admissible statements in a public document. On the other hand, the lack of guaranteed public access ensures that the following are not public documents: government department files, unavailable to the public, in which are recorded certificates authorising persons to operate motor vehicles for profit; regimental records relating to members of the regiment, which are not available to the public; a motor car manufacturer's records: and a car registration book.
9. Page 317. A number of cases implicitly assume that the officer does not have to have verified the truth of the facts recorded in a public document for the statements asserting them to be admissible. The numerous cases dealing with the record maintained by birth, marriage and death registries, which confirm that such registers are public records, illustrate this - obviously the officers receiving such particulars from the public cannot themselves know, nor have they ever been required to verify personally the information supplied for registration.
10. Page 318. The common law recognises that a certified copy of a public document, which concept includes a certified extract from a public register, may be admitted in lieu of the original and that it has the same status as the original.
11. Page 318. Public documents, being an exception on the hearsay rule, are admissible as *prima facie* evidence that their contents - the facts alleged in them - are true. So, for example, a birth certificate (strictly, a certified extract from a register of births, viz., a certified copy of an entry in it) is evidence of the age of the person named in it, quite apart from the

standard statutory provision to this effect.

12. Page 318. Although a certified extract from a public register relating to birth, etc., is evidence of the facts recorded, the document detailing these facts, as supplied by members of the public in order to procure registration, is not itself admissible evidence of the fact, unless it falls within some other exception to the hearsay rule. This consideration indicates that the public document exception, as applied in the context of registers of births, deaths, and marriages, and like registers dependent upon the supply of information by the public, may readily admit false information.
13. Page 319. A meteorological observation as to the atmospheric temperature on a given day at a given time and place, when recorded in a public record, is admissible evidence as to the temperature on this occasion.

- **Document Signature and Authorship**

1. Page 582. At common law, where a private document is sought to be tendered, which document is of a type that is required to be signed by the person creating or adopting it, and in some cases (such as a will) to be attested by a witness or witnesses as well, its due execution must be proven, i.e., it must be authenticated, or validated. Due execution requires proof that the person who purported to sign it did indeed sign it, and (where it is required) that this signature was attested by witnesses. The same rules apply where the original of the document is not tendered, but instead secondary evidence of it is tendered, in the form of a copy, parol evidence, etc.
2. Page 583. A signature may be proven by the signatory or by other evidence, such as testimony by a person who witnessed the signing, by a person familiar with the signature, by reference to a sample of the signature, or by handwriting proven to have been written by the alleged signatory, by admission by the opposing party, and so on. A signature can take a variety of forms and the concept is not confined to the actual writing of his or her name by a person. A signature has been described generally as being "the writing, or otherwise affixing, [of] a person's name, or a mark to represent his name, by himself or by his authority ... with the intention of authenticating a document as being that of, or as binding on, the person whose name or mark is so written or affixed ...." Accordingly, a rubber stamp imprinting a facsimile of a signature, or the writing of a signature purporting to be that of X, by Y acting under X's authority, are signatures at common law.
3. Page 584. In the context of documentary evidence it sometimes becomes necessary or desirable to establish that a given person was the author of a given document containing his or her signature or other handwriting. This may be necessary to establish that the document was executed by this person, or to establish that this person was responsible for forgery, and so on. Such evidence can take a number of forms, such as testimony by the person whose writing it is alleged to be, testimony by another who saw this person create the item of handwriting, or identification of the writing as being that of a person by a witness who is acquainted with the person's handwriting with the disputed writing.
4. Page 584. At common law, where proof of the authorship of a writing is in issue, a specimen of the alleged author's writing may be used as a basis for comparison with the disputed writing, provided a foundation is laid for this comparison, by proof that the specimen is indeed a product of the person's writing. A vital but arbitrary limitation governs this mode of proof, however - the specimen, or standard, must be otherwise connected with the case, in that it is relevant and admissible in relation to another issue apart from that of authorship. Non-expert testimony may be received regarding the issue of whether specimen and the disputed writing conform. Equally, the question may be testified to by an expert in handwriting, this area of knowledge and skill being susceptible to the acquisition of expertise. ... An expert, in testifying as to the question of authorship, can depose to the genuineness of the disputed writing, and is not confined to pointing out the similarities between the writings, notwithstanding that the issue of authorship is ultimately one for tribunal of fact.

5. Page 585. The Criminal Procedure Act 1865 (Eng.) provides that where any writing or signature is in dispute, the same may be compared with any writing or signature, proved to the satisfaction of the court to be genuine, and that this writing or signature together with the evidence of witnesses respecting it, shall be evidence of the genuineness or otherwise of the writing or signature in dispute. The specimen writing (or standard, control or exemplar) must be proven to the court in the first place to be genuine, i.e., a foundation must be laid for the comparison. ... Victorian authority stresses that it must be proven to the trial judge, as a condition of admissibility, that the standard is genuine, given the terms of the standard provision. It is not sufficient for the judge routinely to admit the standard, on the basis that it is for the jury to decide the issue. ... Furthermore, where expert testimony on authorship is received, and in it the expert deposes to uncertainty on the matter, the issue may nevertheless be left with the jury for determination one way or the other.... The trial judge can give the jury a warning in respect of the process of comparing handwriting, where documents are left with it in the absence of expert testimony, when the circumstances require this, but such a warning is not mandatory. He or she should, however, make it clear to the jury that the determination of the question of authorship is solely a matter for it.

- **Some Presumptions Affecting Documents**

1. Page 583. Proof of execution is assisted by a common law presumption to the effect that a document which is proved to be or purports to be over thirty years old and which has been produced from proper custody (in essence, from a place where it might reasonably have been expected to have been stored) was duly executed.
2. Page 587. A contract which is in writing is a conclusive record of the agreement, i.e., it is presumed that the agreement is wholly in writing, unless a contrary intention on the part of the parties can be shown. Others (presumptions) include: the principle that the date of execution recorded on a document is *prima facie* evidence of the date of execution, so that a presumption of this effect arises; the presumption that if a party destroys a document which might have told strongly against him or her, this document was executed by him or her, where execution is in issue; ... the presumption against fraud or wrong, so that it is presumed that an alteration in a deed was made before execution; and the presumption that a document older than 30 years produced from proper custody was fully executed (a period reduced by statute to 20 years in most jurisdictions). ... A document required to be stamped is not admissible as evidence in civil proceedings unless it has been stamped. ... The court can go behind the stated consideration in order to determine whether duty has been paid (as where underpayment is suspected); and in the case of the customary form of provision, the unstamped document is inadmissible for all purposes, including a collateral purpose such as contradicting a witness.
3. Page 289. Declarations made by way of transaction, i.e., a statement intended to effect a transaction (which may or may not have legal effect) are in general not hearsay as narrated in court, given that frequently they will not be tendered to prove the truth of the facts asserted in them, if any, but simply that the transaction was made, or attempted. Examples would include statements by way of offer or acceptance in the contractual situation, where, say, the existence of a contract or its terms is in issue.
4. Page 289. A statement which itself is a fact in issue, and not simply evidence of a fact in issue, will frequently not be hearsay, in that it is not tendered as proof of its contents.

- **Others**

1. Page 36. Other analogous means of storing images, for example, film recorded by a radar apparatus of the movements of ships on a river, sought to be admitted in a case arising from collision between ships, are admissible on the same basis.
2. Page 41. Evidence of a person's fingerprints may be received on the question of his or her identification. Usually, of course, this will be done in criminal proceedings. A person can

properly be convicted of an offence, notwithstanding that the only evidence of the perpetrator is fingerprint evidence, where this evidence taken with the other evidence establishes his or her guilt beyond reasonable doubt. On the other hand, the fact that a person's fingerprints are found at a particular place will not of course necessarily implicate this person in a crime associated with the place.

- **Test or Experiment Results**

1. Page 40. In the absence of statutory provisions facilitating their admission, the results of out-of-court tests and experiments may be adduced into evidence, provided their relevance and authenticity is proven by an appropriate witness. The witness may of course be questioned in great detail as to the procedures employed.

Policy Issues Affecting the Implementation of Public Key Authentication Framework

M.K.F. Lai and M. Anderson

Distribution

DEPARTMENT OF DEFENCE

Science and Technology

Defence Science and Technology Organisation Central

Chief Defence Scientist and members of the	)
DSTO Central Office Executive	) 1 shared copy
Counsellor, Defence Science, London	Cont Sht
Counsellor, Defence Science, Washington	Cont Sht
Senior Defence Scientific Adviser	1 copy
Scientific Adviser POLCOM	1 copy

Aeronautical & Maritime Research Laboratory

Director Aeronautical & Maritime Research Laboratory	1 copy
Chief Air Operations Division	Cont Sht
Chief Maritime Operations Division	Cont Sht

Electronics & Surveillance Research Laboratory

Director Electronics & Surveillance Research Laboratory	Cont Sht
Chief Information Technology Division	1 copy
Chief Electronic Warfare Division	Cont Sht
Chief Guided Weapons Division	Cont Sht
Chief Communications Division	Cont Sht
Chief Land, Space and Optoelectronics Division	Cont Sht
Chief High Frequency Radar Division	Cont Sht
Chief Microwave Radar Division	Cont Sht
Research Leader Command & Control and Intelligence Systems	1 copy
Research Leader Military Computing Systems	1 copy
Research Leader Command, Control and Communications	1 copy
Manager Human Computer Interaction Laboratory	Cont Sht
Head Program and Executive Support	Cont Sht
Head Software Engineering Group	Cont Sht
Head Trusted Computer Systems Group	1 copy
Head Command Support Systems Group	Cont Sht
Head Intelligence Systems Group	Cont Sht
Head Systems Simulation and Assessment Group	Cont Sht
Head Exercise Analysis Group	Cont Sht

Head C3I Systems Engineering Group	Cont Sht
Head Computer Systems Architecture Group	Cont Sht
Head Information Management Group	Cont Sht
Head Information Acquisition & Processing Group	Cont Sht
Authors (M.K.F. Lai)	5 copies
Publications & Publicity Officer ITD	1 copy

Navy

Navy Scientific Adviser	1 copy

Army

Scientific Adviser, Army	1 copy

Air Force

Air Force Scientific Adviser	1 copy

Forces Executive

Director General Force Development (Joint)	1 copy
Director General Force Development (Land)	1 copy
Director General Force Development (Air)	1 copy
Director General Force Development (Sea)	1 copy
Director General Joint Communications and Electronics	1 copy
Deputy Director Network Systems	1 copy

Acquisition and Logistics

Director General Information Management and Communications Engineering	1 copy
Director General Joint Projects Management	1 copy
Department of Defence Information Systems Consultative Group (through Deputy Director Enterprise Applications)	14 copies
Department of Defence Electronic Business Consultative Group (through Deputy Director Enterprise Applications)	25 copies
Deputy Director Enterprise Applications	10 copies

Strategy and Intelligence

Assistant Secretary Scientific Analysis	1 copy
Assistant Secretary Information Security	1 copy

LIBRARIES AND INFORMATION SERVICES

Australian Government Publishing Service	1 copy
Defence Central Library, Technical Reports Centre	1 copy
Manager, Document Exchange Centre, (for retention)	1 copy

Defense Technical Information Service, United States	2 copies
Defence Research Information Centre, United Kingdom	2 copies
Director Scientific Information Services, Canada	1 copy
Library, Ministry of Defence, New Zealand	1 copy
National Library of Australia	1 copy
Defence Science and Technology Organisation Salisbury, Research Library	2 copies
Library Defence Signals Directorate Canberra	1 copy
British Library Document Supply Centre	1 copy
Parliamentary Library of South Australia	1 copy
The State Library of South Australia	1 copy

SPARES

Defence Science and Technology Organisation Salisbury, Research Library	6 copies

This is a blank page.

Department of Defence

DOCUMENT CONTROL DATA SHEET

1. Page Classification	
UNCLASSIFIED	
2. Privacy Marking/Caveat (of document)	
NA	

3a. AR Number	3b. Laboratory Number	3c. Type of Report	4. Task Number
AR-009-248	DSTO-GD-0049	General Document	ADF93/256

5. Document Date	6. Cost Code	8. No. of Pages	44
APRIL 1995	840708	9. No. of Refs.	36

10. Title

POLICY ISSUES AFFECTING THE IMPLEMENTATION OF PUBLIC KEY AUTHENTICATION FRAMEWORK

7. Security Classification

* Document	Title	Abstract
U	U	U

S (Secret) C (Confi) R (Rest) U (Unclass)

* For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

11. Author(s)

M.K.F. Lai & M. Anderson

12. Downgrading/Delimiting Instructions

NA

13a. Corporate Author and Address

Electronics and Surveillance Research Laboratory
PO Box 1500, Salisbury SA 5108

13b. Task Sponsor

HQADF

14. Officer/Position responsible for

Security: SOESRL

Downgrading: CITD

Approval for Release: CITD

15. Secondary Release Statement of this Document

APPROVED FOR PUBLIC RELEASE

16a. Deliberate Announcement

NO LIMITATION

16b. Casual Announcement (for citation in other documents)

[X] No Limitation [ ] Ref. by Author , Doc No. and date only.

17. DEFTEST Descriptors

SIGNATURES
IDENTIFICATION
COMPUTER SECURITY

18. DISCAT Subject Codes

19. Abstract

The main purpose of this paper is to examine a particular issue which impacts Defence business dealings with other government departments and commercial interests and matters related to national security, specifically those of an economic aspect. While there are many security issues which need addressing, we focus on the near term issue of electronic digital signatures and the need for a regulated, country wide mechanism for the legal acceptance of these signatures across multiple businesses and government organs. Finally, we discuss a framework for such a mechanism, namely the Public Key Authentication Framework (PKAF), and expose a number of implications.